



Программный комплекс Систэм Платформ

---

## SePlatform.Data Server 2.1 Модуль Syslog Server

---

Руководство администратора

Редакция  
3. Предварительная

Соответствует версии ПО  
2.1.2

---



© ООО «СИСТЭМ СОФТ», 2022-2024. Все права защищены.

Авторские права на данный документ принадлежат ООО «СИСТЭМ СОФТ». Копирование, перепечатка и публикация любой части или всего документа не допускается без письменного разрешения правообладателя.

# Содержание

---

<b>1. Назначение и принцип работы</b>	<b>4</b>
Протокол Syslog	4
Работа с сообщением в SePlatform.Data Server	4
Работа по TLS/UDP	4
Работа модуля в резерве	5
<b>2. Конфигурирование</b>	<b>6</b>
2.1. Конфигурирование модуля	6
2.2. Добавление сертификатов устройств	9
2.3. Конфигурирование сигналов	9
Генерация событий включена	9
Генерация событий отключена	12
<b>3. Диагностика работы модуля</b>	<b>13</b>
3.1. Статистика	13
3.1.1. Параметры TLS	13
3.1.2. Параметры UDP	14
3.1.3. Дополнительные параметры	15
3.2. Журнал работы модуля	15
<b>4. Приложения</b>	<b>16</b>
Приложение А: Формат сообщений Syslog	16
Приложение В: Генерация событий	20
<b>Список терминов и сокращений</b>	<b>22</b>

# 1. Назначение и принцип работы

Модуль Syslog Server предназначен для диагностики сетевых устройств путём сбора сообщений по протоколу Syslog.

## Протокол Syslog

Протокол Syslog - способ передачи информации о событиях, происходящих в устройстве. Информация передаётся в виде текстовых сообщений.

Сообщение содержит:

- текст события;
- информацию о событии: где и когда оно произошло, важность и пр.



### ПРИМЕЧАНИЕ

Формат сообщения зависит от спецификации, согласно которой формируется сообщение ([стр. 16](#)).

Сообщения передаются по схеме клиент-сервер: при возникновении события устройство формирует сообщение и отправляет его серверу Syslog. Сервер Syslog принимает и обрабатывает сообщение. Правила обработки протоколом не регламентируются и зависят от реализации сервера.

Сообщения передаются в открытом виде (по транспортному протоколу UDP) или с использованием шифрования (по транспортному протоколу TLS).

## Работа с сообщением в SePlatform.Data Server

Модуль Syslog Server принимает сообщения Syslog и записывает в сигналы.

У модуля есть известные форматы сообщений Syslog, все остальные форматы считаются неизвестными модулю ([стр. 16](#)).

Сообщения неизвестного формата могут быть записаны в сигнал только в исходном виде.

Сообщения известного формата могут быть записаны в сигнал в исходном виде либо в преобразованном для генерации динамических событий модулем OPC AE Server: это регулируется настройкой **Генерировать события** модуля Syslog Server.

Если включена настройка **Генерировать события**, то можно распределять сообщения по разным сигналам в соответствии с настроенными фильтрами в свойстве адреса сигналов.

Если сообщения записываются в сигнал в исходном виде, можно разбирать их с помощью модуля логики, формировать строку для генерации динамического события и записывать её в сигнал, который генерирует события.

## Работа по TLS/UDP

При работе с транспортным протоколом TLS сетевое устройство и модуль устанавливают между собой безопасное соединение. Для этого они обмениваются сертификатами. Модуль принимает сообщения только

от тех сетевых устройств, сертификат которых есть в папке доверенных сертификатов.

При работе с транспортным протоколом UDP модуль принимает сообщения от любых сетевых устройств.

## Работа модуля в резерве

В резерве модуль не принимает сообщения.

## 2. Конфигурирование

Для конфигурирования модуля и сигналов потребуется следующая информация:

- список сетевых устройств, от которых нужно принимать сообщения Syslog;
- для каждого сетевого устройства - в каком виде сообщения будут записаны: в исходном или в преобразованном для генерации событий;
- для каждого сетевого устройства - сообщения передаются по протоколу UDP (в открытом виде) или TLS (в зашифрованном виде);
- (опционально) для сетевых устройств, передающих сообщения по TLS - сертификат устройства.

Список сетевых устройств нужно разбить на группы, по признакам:

- в каком виде сообщения будут записаны: в исходном/преобразованном;
- сообщения передаются в открытом/зашифрованном виде.

	Сообщения записываются в исходном виде	Сообщения записываются в преобразованном виде
UDP	Группа 1	Группа 2
TCL	Группа 3	Группа 4

Для каждой группы нужно добавить свой экземпляр модуля Syslog Server и конфигурировать его независимо от остальных (включая конфигурирование сигналов).

### 2.1. Конфигурирование модуля

1. Добавьте в состав конфигурации SePlatform.Data Server модуль Syslog Server.

Добавление модуля

Имя	Описание
OPC UA Client	Коммуникационный модуль предназначенный для передачи данных по протоколу OPC UA
Syslog Server	Модуль сбора сообщений Syslog
Модуль рассылки событий	Модуль для рассылки уведомлений по электронной почте

Добавить

2. В группе **Общие** параметру **Активность** установите значение «Да», чтобы модуль запускался при запуске/перезапуске SePlatform.Data Server. Для остальных параметров можно оставить значения по умолчанию.

1. Общие	
Имя модуля	Syslog Server
Идентификатор модуля	Syslog Server
Активность	Да
Уровень трассировки в журнал приложений	Информационные сообщения
Вести журнал работы модуля	Нет
Размер журнала работы модуля, МБ	10
Количество дополнительных журналов работы	1

### Общие параметры

Параметр	Описание
Имя модуля	Название модуля
Идентификатор модуля	Идентификатор модуля
Активность	Активность модуля: <ul style="list-style-type: none"> <li>➤ «Да» - модуль запущен</li> <li>➤ «Нет» - модуль остановлен</li> </ul>
Уровень трассировки в журнал приложений	<p>Типы сообщений, которые фиксируются в журнал приложений:</p> <ul style="list-style-type: none"> <li>➤ «Предупреждения и аварийные сообщения» - логические ошибки, ошибки работы модуля. Предупреждения содержат не критичные ошибки. Аварийные сообщения информируют об ошибках, которые влияют на работоспособность службы</li> <li>➤ «Информационные сообщения» - сообщения, которые показывают основную информацию о работе модуля</li> <li>➤ «Отладочные сообщения» - сообщения, которые наиболее детально отражают информацию о работе модуля</li> </ul> <p>Вышестоящий уровень входит в состав нижестоящего: если выбрано «Информационные сообщения», то в журнал фиксируются «Предупреждения и аварийные сообщения» и «Информационные сообщения»</p>
Вести журнал работы модуля	<p>Ведётся ли журнал работы модуля:</p> <ul style="list-style-type: none"> <li>➤ «Да»</li> <li>➤ «Нет»</li> </ul>
Размер журнала работы модуля, МБ	<p>Ограничение на размер файла журнала работы модуля в мегабайтах.</p> <p>При достижении максимального размера создается новый файл, копия старого файла хранится на рабочем диске</p>
Количество дополнительных журналов работы	<p>Количество файлов заполненных журналов работы модуля.</p> <p>Минимальное значение - 1, максимальное - 255</p>

3. В группе **Дополнительные**:

3.1. Установите необходимое значение параметра **Генерировать события**:

- «Да» - сообщения Syslog будут преобразованы к виду конструкции для генерации динамического события. Это применимо только для сообщений, которые имеют известный модулю формат.
- «Нет» - сообщения Syslog будут записаны в исходном виде. Это применимо для любых форматов сообщений.

### 3.2. Укажите Транспортный протокол и Порт:

- для протокола UDP - порт «514»;
- для протокола TLS - порт «6514».



#### ОБРАТИТЕ ВНИМАНИЕ

Если в конфигурацию SePlatform.Data Server добавлено несколько экземпляров модуля Syslog Server, то каждому необходимо указать уникальный порт.

3.3. Если выбран транспортный протокол TLS, то укажите сертификат сервера и приватный ключ. Для этого укажите абсолютный путь к файлу или только имя файла, если он находится в папке SePlatform.Data Server:

- сертификат сервера: <папка SePlatform.Data Server>\Certificates\certs
- приватный ключ сервера: <папка SePlatform.Data Server>\Certificates\private



#### ПРИМЕЧАНИЕ

Сертификат сервера и приватный ключ создаются в процессе установки SePlatform.Data Server.

2. Дополнительные	
Генерировать события	Да
Транспортный протокол	TLS
Порт	0
Путь к сертификату сервера	C:\Program Files\SePlatform\SePlatform.Server\Server\Certificates\certs
Путь к приватному ключу сервера	C:\Program Files\SePlatform\SePlatform.Server\Server\Certificates\certs

Параметр	Описание
Генерировать события	<p>Записывать значение в виде, пригодном для генерации событий:</p> <ul style="list-style-type: none"> <li>➤ «Нет» - сообщение будет записано в том виде, в котором получено (со всеми полями);</li> <li>➤ «Да» - сообщение будет записано в формате:</li> </ul> <pre>&lt;Subcondition Type="Dynamic" Message="MSG" /&gt;</pre> <p>где MSG - поле <b>MSG</b> в полученном сообщении.</p> <p>Формат предназначен для автоматической генерации события при его записи в сигнал.</p>
Транспортный протокол	<p>Тип транспортного протокола, используемого для передачи сообщений Syslog:</p> <ul style="list-style-type: none"> <li>➤ «TLS»</li> <li>➤ «UDP»</li> </ul>
Порт	Порт приема данных



Параметр	Описание
Путь к сертификату сервера	Абсолютный путь к сертификату сервера или имя сертификата сервера. Используется только при работе по протоколу TLS
Путь к приватному ключу сервера	Абсолютный путь к приватному ключу сервера или имя приватного ключа сервера. Используется только при работе по протоколу TLS

## 2.2. Добавление сертификатов устройств



### ОБРАТИТЕ ВНИМАНИЕ

Добавлять сертификаты нужно только при работе с транспортным протоколом TLS.

При работе с транспортным протоколом TLS, чтобы сервер принимал сообщения от сетевого устройства, нужно добавить сертификат этого устройства в папку доверенных сертификатов <папка SePlatform.Data Server>\Certificates\TrustedPeers\certs. Добавлять сертификаты можно при конфигурировании или в процессе работы сервера.

При попытке установить соединение устройство отправляет серверу свой сертификат. Если сертификат не будет найден в папке доверенных сертификатов, он будет сохранён в папке отклонённых сертификатов <папка SePlatform.Data Server>\Certificates\Rejected\certs. При каждой попытке соединения будет сохранена новая копия сертификата. Чтобы сделать устройство доверенным, переместите любую копию его сертификата в папку доверенных сертификатов.

## 2.3. Конфигурирование сигналов

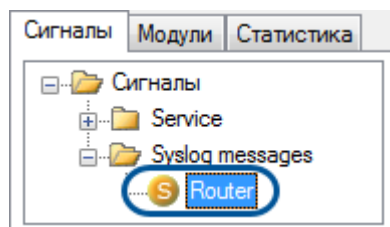
Конфигурирование сигналов различается в зависимости от того, включена настройка модуля **Генерировать события** или нет.

### Генерация событий включена

Для каждого сетевого устройства, от которого нужно принимать сообщения:

1. Создайте в дереве сигналов сигнал типа String.

Сигнал может находиться в любом месте дерева сигналов.

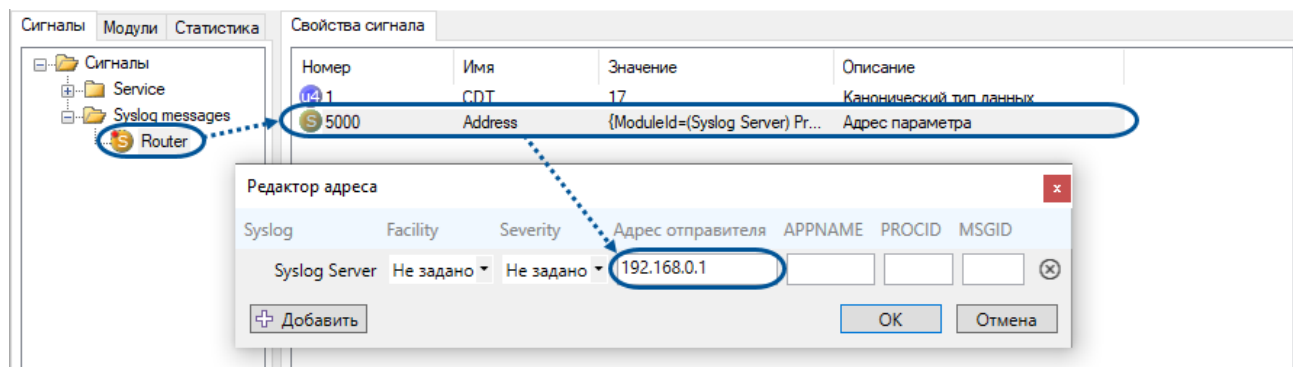


2. Для сигнала настройте получение сообщений Syslog от устройства:

2.1. Добавьте сигналу свойство **5000 (Address)** типа String.

2.2. В открывшемся окне **Редактор адреса** добавьте модуль Syslog Server.

2.3. В параметре **Адрес отправителя** укажите адрес сетевого устройства.



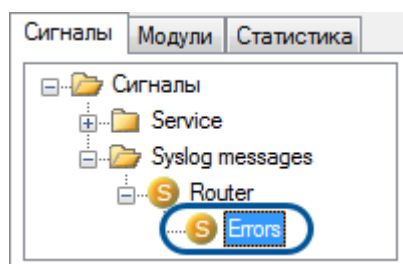
#### ОБРАТИТЕ ВНИМАНИЕ

Чтобы принимать сообщения от любых сетевых устройств, оставьте поле **Адрес отправителя** пустым: в сигнал будут записываться сообщения от устройств, для которых не созданы отдельные сигналы.

3. Для сигнала настройте генерацию динамических событий ([стр. 20](#)).

Сообщения можно фильтровать. Это нужно, например, чтобы отделить сообщения об ошибках от прочих сообщений. Для этого:

1. Добавьте в дерево сигналов новый сигнал типа String.

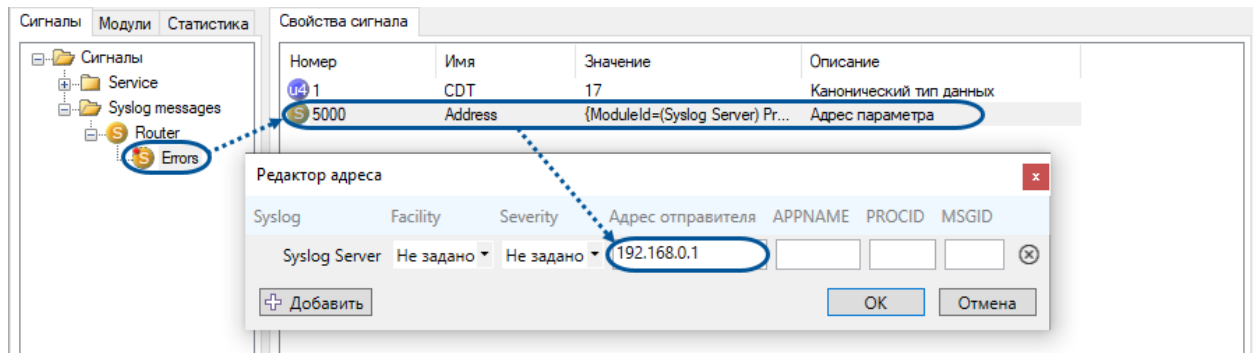


2. Для сигнала настройте получение сообщений Syslog от устройства:

2.1. Добавьте сигналу свойство **5000 (Address)** типа String.

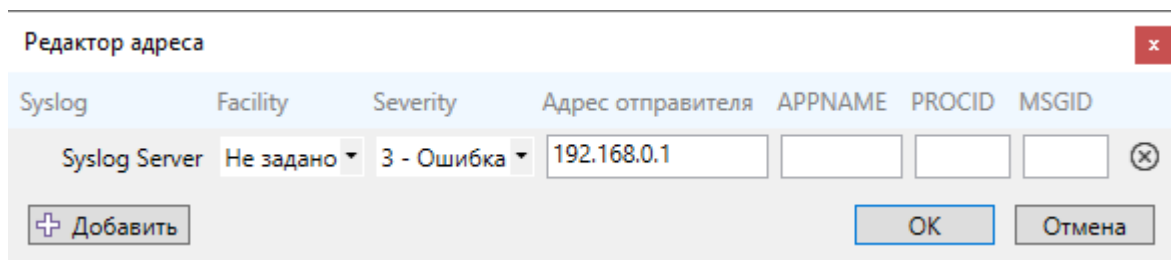
2.2. В открывшемся окне **Редактор адреса** добавьте модуль Syslog Server.

2.3. В параметре **Адрес отправителя** укажите адрес сетевого устройства.



2.4. В остальных полях укажите значения необходимых параметров фильтрации:

- Facility
- Severity
- APPNAME
- PROCID
- MSGID



Каждое сообщение записывается в один сигнал. Если для записи сообщения подходит несколько сигналов, проверяется, какие поля указаны у каждого сигнала. Приоритет полей (от наибольшего к наименьшему):

- Адрес отправителя;
- Facility;
- Severity;
- APPNAME;
- PROCID;
- MSGID.

Для каждого поля проверяется:

- если поле указано или не указано у всех сигналов → переходим к следующему полю;
- если поле указано не у всех сигналов → выбираем из сигналов, у которых поле указано.



#### ПРИМЕР

Пусть есть два подходящих сигнала для записи сообщения:

- у первого задано поле **Адрес отправителя**;
- у второго указаны поля **Адрес отправителя** и **Severity**.

Сообщение будет записано во второй сигнал, т.к. у него указано больше полей.



## ПРИМЕР

Пусть есть два подходящих сигнала для записи сообщения:

- у первого задано поле **Адрес отправителя**;
- у второго указаны поля **Facility** и **Severity**.

Сообщение будет записано в первый сигнал, т.к. поле **Адрес отправителя** имеет наибольший приоритет.



## ПРИМЕР

Пусть есть два подходящих сигнала для записи сообщения:

- у первого указаны поля **Адрес отправителя** и **Facility**;
- у второго указаны поля **Адрес отправителя** и **Severity** и **APPNAME**.

Сообщение будет записано в первый сигнал, т.к. поле **Facility** имеет больший приоритет, чем поля **Severity** и **APPNAME**.

## Генерация событий отключена

1. Создайте сигнал для генерации событий:
  - 1.1. Создайте сигнал типа String.
  - 1.2. Для сигнала настройте генерацию динамических событий.
2. Создайте сигнал для записи принятых сообщений:
  - 2.1. Создайте сигнал типа String.
  - 2.2. Добавьте сигналу свойство **5000 (Address)** типа String.
  - 2.3. В открывшемся окне **Редактор адреса** добавьте модуль Syslog Server. Значения полей указывать не нужно
3. Настройте разбор принятых сообщений с помощью модуля логики.

Один из способов разбора:

- 3.1. Сигналу, в который записываются сообщения, добавьте свойство **777012** типа String. Код, описанный в свойстве, выполняется при изменении значения сигнала.
- 3.2. В свойстве опишите код, который будет с помощью строковых функций разбирать сообщения. В коде, после того как сообщение разобрано, нужно записать его в сигнал, генерирующий события. Записывать нужно в таком виде, чтобы при записи генерировалось динамическое событие с текстом сообщения:

```
<Subcondition Type="Dynamic" Message="MSG" />
```



## ОБРАТИТЕ ВНИМАНИЕ

Чтобы код выполнялся, добавьте и активируйте модуль логики.

## 3. Диагностика работы модуля

### 3.1. Статистика

Статистическая информация о работе модуля отображается на вкладке **Статистика** сервисного приложения Конфигуратор, а также в сервисном приложении Статистика.

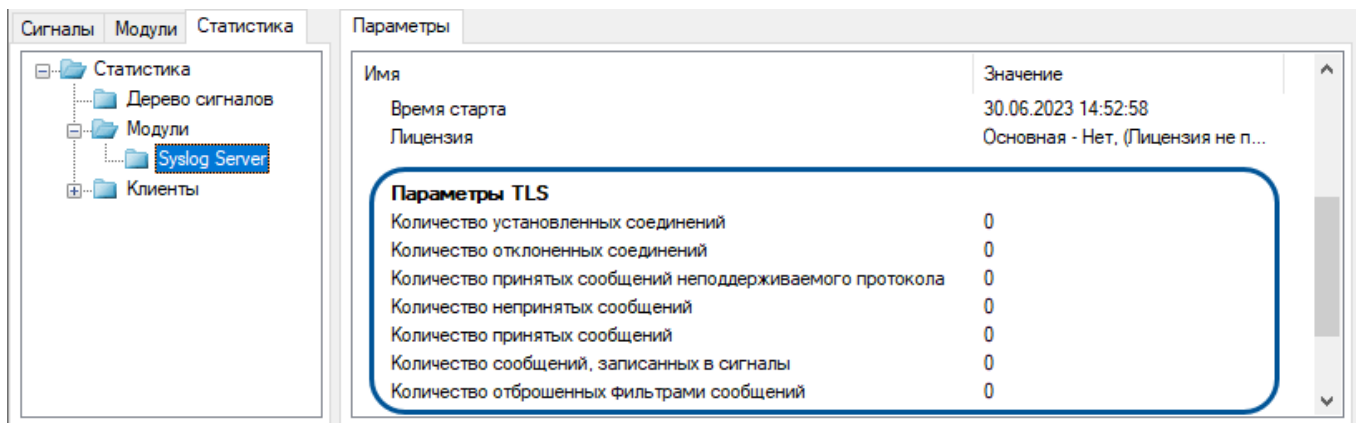
Чтобы просмотреть параметры статистики модуля, подключитесь к SePlatform.Data Server и выберите модуль в дереве статистики.

#### 3.1.1. Параметры TLS



##### ОБРАТИТЕ ВНИМАНИЕ

Параметры TLS отображаются, если в настройках модуля выбран транспортный протокол TLS.



Параметр	Описание
Количество установленных соединений	Количество соединений с доверенными устройствами, установленных с момента начала работы сервера
Количество отклоненных соединений	Количество попыток соединений от устройств, сертификат которых отсутствует в папке доверенных сертификатов
Количество принятых сообщений неподдерживаемого протокола	Количество полученных модулем сообщений, неподдерживаемого протокола
Количество непринятых сообщений	Количество сообщений, полученных модулем, которые не могут быть успешно разобраны. Сообщение будет успешно разобрано, если его формат соответствует спецификации RFC 5424.

Параметр	Описание
Количество принятых сообщений	Количество полученных и успешно разобранных модулем сообщений
Количество сообщений записанных в сигналы	Количество полученных модулем сообщений, которые были записаны в сигналы сервера
Количество отброшенных фильтрами сообщений	Количество полученных и разобранных модулем сообщений, которые не соответствуют ни одному настроенному в сервере сигналу. Для каждого такого сообщения в журнал работы модуля записывается уведомление об отсутствии в сервере сигнала, подходящего для записи полученного сообщения

### 3.1.2. Параметры UDP

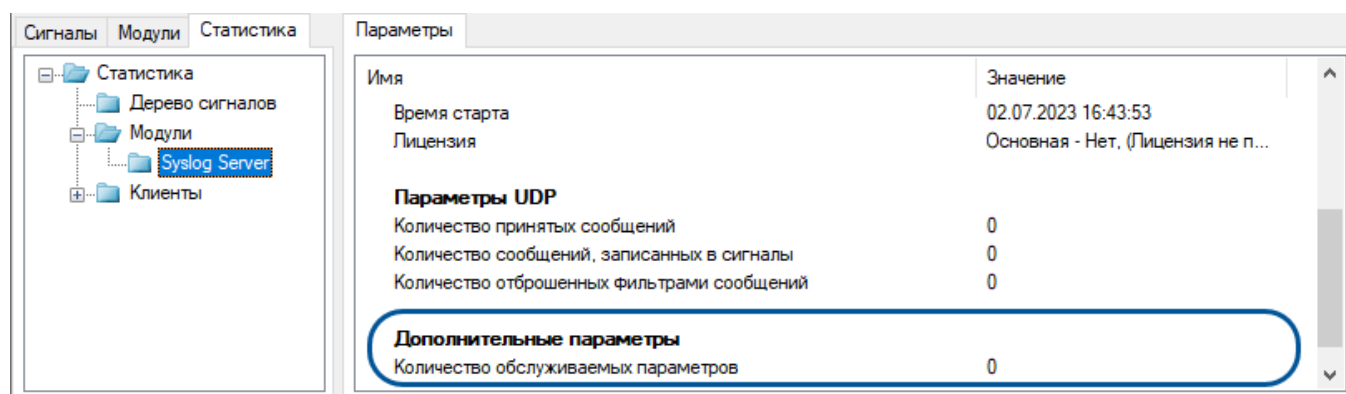


#### ОБРАТИТЕ ВНИМАНИЕ

Параметры UDP отображаются, если в настройках модуля выбран транспортный протокол UDP.

Параметр	Описание
Количество принятых сообщений	Количество сообщений Syslog, полученных модулем с начала работы сервера
Количество сообщений записанных в сигналы	Количество полученных модулем сообщений, которые были записаны в сигналы сервера
Количество отброшенных фильтрами сообщений	Количество полученных модулем сообщений, не соответствующих ни одному настроенному в сервере сигналу. Для каждого такого сообщения в журнал работы модуля записывается уведомление об отсутствии в сервере сигнала, подходящего для записи полученного сообщения

### 3.1.3. Дополнительные параметры



Параметр	Описание
Количество обслуживаемых параметров	Количество сигналов, поставленных на обслуживание модулю

## 3.2. Журнал работы модуля

Журнал работы модуля сохраняется в файл <имя модуля>.aplog по умолчанию:

- в папке C:\Program Files\SePlatform\SePlatform.Server\Logs, если SePlatform.Data Server функционирует в ОС Windows;
- в директории /opt/SePlatform/Logs, если SePlatform.Data Server функционирует в ОС семейства Linux.

Для просмотра журнала работы модуля воспользуйтесь сервисным приложением Просмотрщик лога кадров.

В журнал работы модуля записываются:

- все полученные сообщения Syslog;
- уведомления об отсутствии в сервере сигнала, подходящего для записи полученного сообщения;
- при работе по протоколу TLS - уведомления о неверном формате полученного сообщения.

## 4. Приложения

### Приложение А: Формат сообщений Syslog

Модуль Syslog Server поддерживает следующие форматы сообщений Syslog :

- RFC 5424;
- RFC 3164.

#### RFC 5424

Сообщение Syslog в формате RFC 5424 имеет следующую структуру:

```
<PRI>VERSION TIMESTAMP HOSTNAME APPNAME PROCID MSGID [STRUCTURED-DATA] MSG
```

Diagram illustrating the structure of a Syslog message in RFC 5424 format. The message is: `<165>1 2003-10-11T22:14:15.003Z somedomain.com evntslg 666 ID47 [SDID@32473 iut="3" eventSource="Application" eventID="1011"] Log entry...`. The fields are labeled as follows: **PRI** (green), **VERSION** (blue), **TIMESTAMP** (green), **HOSTNAME** (blue), **APP-NAME** (green), **PROCID** (blue), **MSGID** (green). The **STRUCTURED-DATA** field is highlighted in red and labeled **STRUCTURED-DATA** in red. The **MSG** field is labeled **MSG** in blue.

При передаче сообщений Syslog по протоколу TLS в начале сообщения указывается его размер:

```
LENGTH <PRI>VERSION TIMESTAMP HOSTNAME APPNAME PROCID MSGID [STRUCTURED-DATA] MSG
```

Diagram illustrating the structure of a Syslog message in RFC 5424 format, including the **LENGTH** field. The message is: `139 <165>1 2018-04-23T05:14:15.003Z somedomain.com evntslg 666 ID47 [SDID@32473 iut="3" eventSource="Application" eventID="1011"] Log entry...`. The fields are labeled as follows: **LENGTH** (blue), **PRI** (green), **VERSION** (blue), **TIMESTAMP** (green), **HOSTNAME** (blue), **APP-NAME** (green), **PROCID** (blue), **MSGID** (green). The **STRUCTURED-DATA** field is highlighted in red and labeled **STRUCTURED-DATA** in red. The **MSG** field is labeled **MSG** in blue.

Согласно спецификации RFC 5424 в сообщении могут быть не указаны значения следующих полей:

- **HOSTNAME**;
- **APPNAME**;
- **PROCID**;
- **MSGID**.

Вместо отсутствующего значения в поле должен быть указан символ «-».



## RFC 3164



### ОБРАТИТЕ ВНИМАНИЕ

Сообщения Syslog в формате RFC 3164 передаются только по транспортному протоколу UDP.

Сообщение Syslog в формате RFC 3164 имеет следующую структуру:

```
<PRI> TIMESTAMP HOSTNAME APPNAME [PROCID]:MSG
```

**PRI** **TIMESTAMP** **HOSTNAME** **APPNAME** **PROCID** **MSG**

<34>Oct 11 22:14:15 mymachine su[10]: Log entry...

Согласно спецификации RFC 3164 в сообщении могут быть не указаны значения любых полей. В этом случае значения соответствующих полей будут отсутствовать в структуре сообщения (допускается передача пустого сообщения, не содержащего ни одного символа):

- если в сообщении не указано значение «TIMESTAMP», то в качестве значения поля используется момент получения сообщения;
- если в сообщении не указано значение «PRI», то в качестве значения поля **PRI** используется значение «41» (Facility - «5», Severity - «1»);
- при отсутствии значений прочих полей, в качестве значения этих полей используется пустая строка.

Формату RFC 3164 соответствуют любые сообщения, которые могут быть получены: если при попытке разобрать отдельные поля в полученном сообщении произойдёт ошибка, то вся строка сообщения будет использоваться в качестве значения поля **MSG**.

## Описание полей сообщений Syslog

Поле	Описание
<b>LENGTH</b>	Количество символов в сообщении. Указывается только в сообщениях, передаваемых по протоколу TLS

Поле	Описание																																				
<b>PRI</b>	<p>Приоритет. Содержит два значения: Facility (субъект, сформировавший сообщение) и Severity (уровень важности сообщения). Severity принимает значения от «0» до «7», Facility - от «0» до «23». Значение PRI вычисляется как <math>PRI = Facility * 8 + Severity</math>.</p> <table> <tr> <td>Facility</td><td>Severity:</td></tr> <tr> <td>0 - Ядро операционной системы</td><td>0 - Авария, система неработоспособна</td></tr> <tr> <td>1 - ПО пользователя</td><td>1 - Тревога, система требует немедленного вмешательства</td></tr> <tr> <td>2 - Почтовая система</td><td>2 - Состояние системы критическое</td></tr> <tr> <td>3 - Системные службы</td><td>3 - Сообщения об ошибках</td></tr> <tr> <td>4 - Сообщения безопасности/авторизации</td><td>4 - Предупреждения о возможных проблемах</td></tr> <tr> <td>5 - Собственные сообщения syslogd</td><td>5 - Сообщения о нормальных, но важных событиях</td></tr> <tr> <td>6 - Подсистема печати</td><td>6 - Информационные сообщения</td></tr> <tr> <td>7 - Подсистема новостных групп</td><td>7 - Отладочные сообщения</td></tr> <tr> <td>8 - Подсистема UUCP</td><td></td></tr> <tr> <td>9 - Службы времени</td><td></td></tr> <tr> <td>10 - Сообщения безопасности/авторизации</td><td></td></tr> <tr> <td>11 - Служба FTP</td><td></td></tr> <tr> <td>12 - Подсистема NTP</td><td></td></tr> <tr> <td>13 - Сообщения аудита</td><td></td></tr> <tr> <td>14 - Аварийные сообщения</td><td></td></tr> <tr> <td>15 - Службы времени 2</td><td></td></tr> <tr> <td>16-23 - локальное происхождение 0-7</td><td></td></tr> </table>	Facility	Severity:	0 - Ядро операционной системы	0 - Авария, система неработоспособна	1 - ПО пользователя	1 - Тревога, система требует немедленного вмешательства	2 - Почтовая система	2 - Состояние системы критическое	3 - Системные службы	3 - Сообщения об ошибках	4 - Сообщения безопасности/авторизации	4 - Предупреждения о возможных проблемах	5 - Собственные сообщения syslogd	5 - Сообщения о нормальных, но важных событиях	6 - Подсистема печати	6 - Информационные сообщения	7 - Подсистема новостных групп	7 - Отладочные сообщения	8 - Подсистема UUCP		9 - Службы времени		10 - Сообщения безопасности/авторизации		11 - Служба FTP		12 - Подсистема NTP		13 - Сообщения аудита		14 - Аварийные сообщения		15 - Службы времени 2		16-23 - локальное происхождение 0-7	
Facility	Severity:																																				
0 - Ядро операционной системы	0 - Авария, система неработоспособна																																				
1 - ПО пользователя	1 - Тревога, система требует немедленного вмешательства																																				
2 - Почтовая система	2 - Состояние системы критическое																																				
3 - Системные службы	3 - Сообщения об ошибках																																				
4 - Сообщения безопасности/авторизации	4 - Предупреждения о возможных проблемах																																				
5 - Собственные сообщения syslogd	5 - Сообщения о нормальных, но важных событиях																																				
6 - Подсистема печати	6 - Информационные сообщения																																				
7 - Подсистема новостных групп	7 - Отладочные сообщения																																				
8 - Подсистема UUCP																																					
9 - Службы времени																																					
10 - Сообщения безопасности/авторизации																																					
11 - Служба FTP																																					
12 - Подсистема NTP																																					
13 - Сообщения аудита																																					
14 - Аварийные сообщения																																					
15 - Службы времени 2																																					
16-23 - локальное происхождение 0-7																																					
<b>VERSION</b>	Версия протокола																																				
<b>TIMESTAMP</b>	Метка времени сообщения																																				
<b>HOSTNAME</b>	IP-адрес или сетевое имя устройства, сгенерировавшего сообщение																																				
<b>APP-NAME</b>	Идентификатор устройства или приложения, сгенерировавшего сообщение																																				
<b>PROCID</b>	Позволяет регистрировать перерывы в потоке данных и обычно используется в качестве идентификатора процесса																																				
<b>MSGID</b>	Идентификатор типа сообщения																																				
<b>STRUCTURED-DATA</b>	Структурированные данные. В работе модуля Syslog Server не используются																																				
<b>MSG</b>	Текст сообщения																																				

Поля сообщений Syslog используются следующим образом:

- поля **MSG** и **TIMESTAMP** используются при формировании VQT значения, записываемого в сигнал;
- поле **HOSTNAME** используется при поиске сигнала, предназначенного для записи сообщений от устройства, указанного в этом поле;

- поля **PRI**, **APP-NAME**, **PROCID**, **MSGID** используются при поиске сигнала, имеющего соответствующие параметры фильтрации.

## Приложение В: Генерация событий

Генерацию событий в сервере выполняет модуль OPC AE Server. События генерируются при записи сообщений Syslog в настроенные сигналы.

Для полученного сообщения Syslog в сервере не будет сгенерировано событие в следующих случаях:

- если в сервере нет подходящего сигнала для записи сообщения;
- если для сигнала, в который сообщение было записано, не настроена генерация событий.

### Настройка

Для каждого сигнала, в который записываются сообщения Syslog, необходимо:

- настроить в свойствах родительской папки условие генерации события. Тип условия - «Dynamic»
- поставить сигнал на обслуживание модулю OPC AE Server с параметром «Conditions=(CONDITION\_NAME)», где CONDITION\_NAME - это название условия, указанное в свойствах папки.



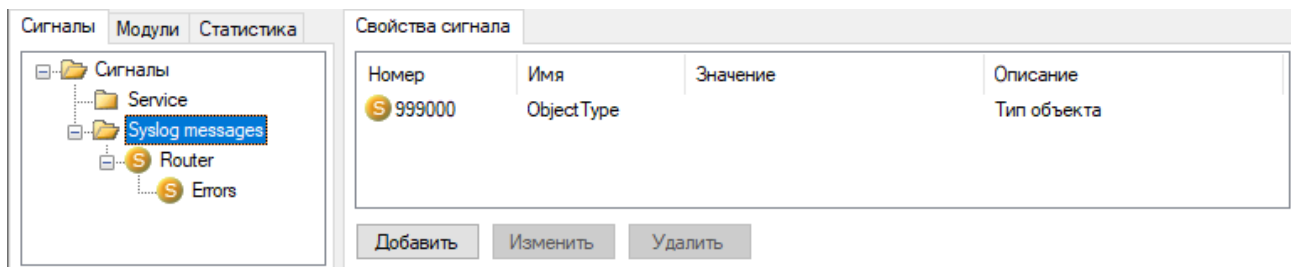
#### ОБРАТИТЕ ВНИМАНИЕ

Данный список содержит общее описание необходимых действий по настройке генерации событий. Подробное описание выполняемых настроек приведено в документации на модуль OPC AE Server.

### Пример

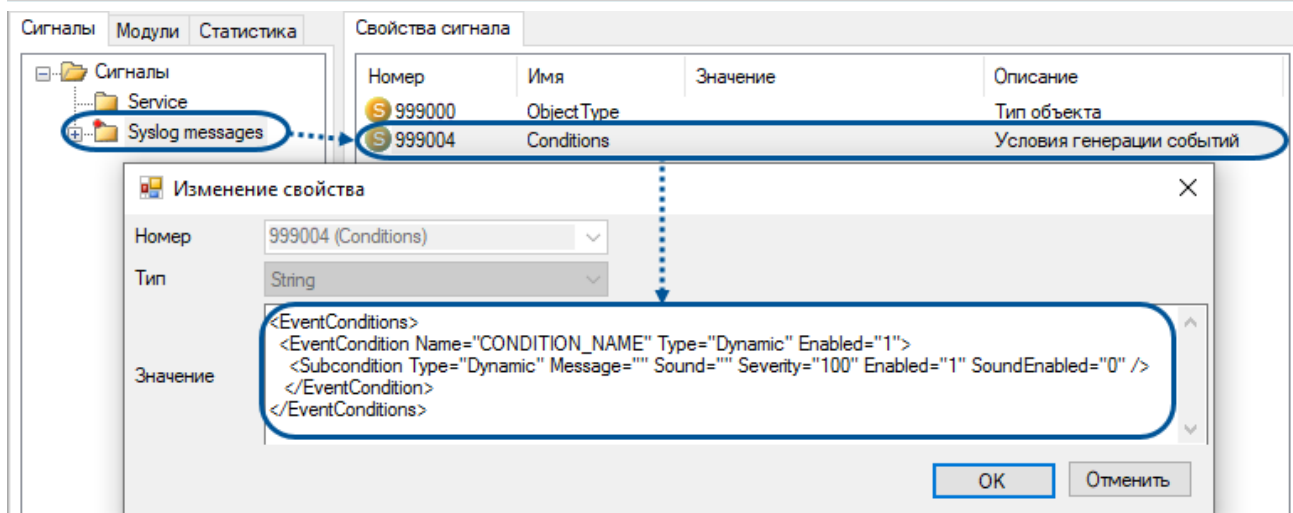
Выполните следующие действия:

1. Родительской папке сигнала добавьте свойство **999000 (ObjectType)** без значения.

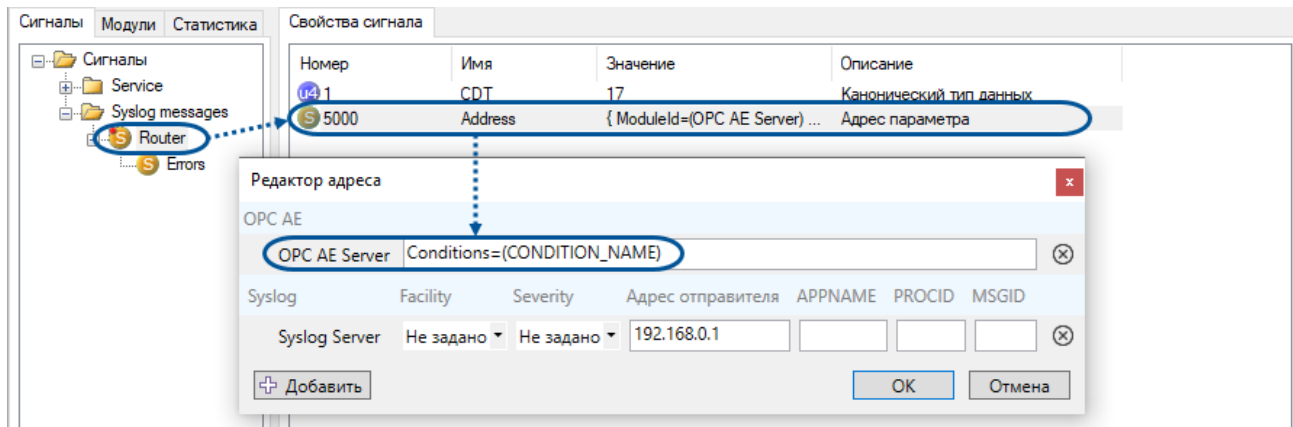


2. Родительской папке сигнала добавьте свойство **999004 (Conditions)**, в значении которого укажите следующую XML-конструкцию:

```
<EventConditions>
  <EventCondition Name="CONDITION_NAME" Type="Dynamic" Enabled="1">
    <Subcondition Type="Dynamic" Message="" Sound="" Severity="100" Enabled="1"
SoundEnabled="0" />
  </EventCondition>
</EventConditions>
```



3. У сигнала в свойстве **5000 (Address)** добавьте модуль OPC AE Server с параметром «Conditions=(CONDITION\_NAME)».



## Список терминов и сокращений

---

<b>SePlatform.Data Server</b>	Сервер ввода/вывода.
<b>Syslog</b>	Протокол отправки и регистрации текстовых сообщений о происходящих в сетевых устройствах событиях.
<b>TLS (Transport Layer Security)</b>	Криптографический транспортный протокол, который обеспечивает защищенную передачу данных.
<b>UDP (User Datagram Protocol)</b>	Транспортный протокол, который передает данные без предварительной организации надежного канала связи.
<b>VQT</b>	Основные свойства сигнала согласно стандарту OPC: Value (значение), Quality (качество), Timestamp (метка времени).